REMARKS

The Decision on Appeal mailed September 18, 2008 has been received and carefully considered. In this response, independent claims 1, 4, 5, 7, 10, and 11 have been amended. No new matter has been added. Entry of the amendments to claims 1, 4, 5, 7, 10, and 11 is respectfully requested. Reconsideration of the current rejections in the present application is also respectfully requested based on the following remarks.[1]

I. THE ANTICIPATION REJECTION OF CLAIMS

On pages 6-9 of the Decision on Appeal, the rejection of claims 1, 2, 4-8, and 10-12 under 35 U.S.C. § 102(e) as being anticipated by Perlman et al. (U.S. Patent No. 6,546,486, hereinafter "Perlman") has been affirmed. In light of the current amendments to independent claims 1, 4, 5, 7, 10, and 11, this affirmation of the rejection is hereby respectfully traversed.

[1] As Applicants' remarks with respect to the Examiner's rejections are sufficient to overcome these rejections, Applicants' silence as to assertions made by the Examiner in the Office Action or certain requirements that may be applicable to such rejections (e.g., assertions regarding dependent claims, whether a reference constitutes prior art, whether references are legally combinable for obviousness purposes) is not a concession by Applicants that such assertions are accurate or such requirements have been met, and Applicants reserve the right to analyze and dispute such in the future.

Under 35 U.S.C. § 102, the Patent Office bears the burden of presenting at least a prima facie case of anticipation. In re King, 801 F.2d 1324, 1326 (Fed. Cir. 1986). Anticipation requires that a prior art reference disclose, either expressly or under the principles of inherency, each and every element of the claimed invention. Celeritas Tech., Ltd., v. Rockwell Int'l Corp., 150 F.3d 1354, 1361 (Fed. Cir. 1998). The prior art reference must disclose all of the claim elements arranged or combined in the same way as recited in the claim. Net MoneyIN, Inc. v. VeriSign, Inc. (CAFC Appeal No. 2007-1565) (Fed. Cir. 2008). "In addition, the prior art reference must be enabling." Akzo N.V. v. U.S. International Trade Commission, 808 F.2d 1471, 1479 (Fed. Cir. 1986), cert. denied, 482 U.S. 909 (1987). That is, the prior art reference must sufficiently describe the claimed invention so as to have placed the public in possession of it. In re Donohue, 766 F.2d 531, 533 (Fed. Cir. 1985). Such possession is effected only if one of ordinary skill in the art could have combined the disclosure in the prior art reference with his/her own knowledge to make the claimed invention. Id.. As stated in MPEP § 2131, "[a] claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art

reference." Verdegaal Bros. v. Union Oil Co. of California, 814 F.2d 628, 631 (Fed. Cir. 1987).

Regarding independent claim 1, the Decision on Appeal construes the "detecting" limitation as being able to "occur in the host, remote, or firewall." Accordingly, the Decision on Appeal asserts that Perlman discloses the claimed invention.

However, in light of the amendments to claim 1, Applicants respectfully disagree. Specifically, Applicants have amended the claim 1 to show that the steps of the method occur at a firewall. For example, the step of "detecting" occurs "**at a firewall**" and "**is initiated by the firewall**" (emphasis added). As a result, Perlman does not teach at least these limitation.

By contrast, Perlman requires a host computer sending an encrypted message to also send the encryption key. For example, column 6, lines 7-13 of Perlman recites:

> The system **starts** by negotiating a message key 204 (a session key) and a security association 210 between source 102 and destination 110 (step 402). This negotiation process may include authenticating source 102 to destination 110 and authenticating destination 110 to source 102. The negotiated message key 204 **and** security association 210 are **then** sent to firewall 106 in a secure manner by either source 102 or destination 110 (step 404).

In other words, Perlman's firewall has no way of identifying encrypted messages. Perlman's firewall does not to initiate the detection. Rather, Perlman's system relies on the sender (e.g.,

the source 102 or the destination 110) to alert the firewall about encrypted messages and to deliver the key to the firewall as part of the messages being sent. This is clearly distinguishable from "detecting, at a firewall, an exchange of a first encryption key between a host device and a remote device...wherein detecting the exchange is initiated by the firewall," as claimed (emphasis added).

This is important because in Perlman's system, if the sender (e.g., the source 102 or the destination 110) is a non-trusted party residing outside the firewall, there can be no way for Perlman's system to force or request the non-trusted party to deliver the encryption keys. In fact, as described above, there is no way that Perlman's firewall even knows that the message is encrypted. Perlman's system presupposes that transmissions start within a trusted (or protected) network and that the computers (e.g., source 102 or destination 110) initiating the exchange will follow rules and deliver encryption keys. Thus, with Perlman's system, there is no mechanism to enforce the firewall security policy for incoming messages from an external non-trusted user. Accordingly, Perlman's firewall does not initiate detection of an exchange of a first encryption key.

Furthermore, since Perlman's firewall does not initiate detection of an exchange of a first encryption key, Perlman also does not teach the step of "**requesting, at the firewall,...the first encryption key from the host device**, wherein the first encryption key is sent under the protection of the second encryption key and in **accordance with the second security policy**," as expressly recited in claim 1, as amended (emphasis added). Because the firewall in Perlman's system relies/trusts the source 102 or destination 110, there is no mechanism to enforce the firewall security policy for incoming messages from a non-trusted external user. Since claim 1, as amended, clearly shows that a firewall detects encryption key exchange sessions, devices outside the trusted network initiating the session would work equally well with devices within the trusted network initiating the session. Because all devices (e.g., host, remote) initiating encrypted sessions are not assumed to be trustworthy, the firewall may therefore force (e.g., by requesting) such devices to securely render keys to the firewall for policy enforcement.

Accordingly, it is respectfully submitted that claim 1 is allowable over Perlman because Perlman does not teach each and every limitation of claim 1.

Regarding claims 4, 5, 7, 10, and 11, these claims, as amended, recite subject matter related to claim 1. Thus, the arguments set forth above with respect to claim 1 are equally applicable to claims 4, 5, 7, 10, and 11. Accordingly, is it respectfully submitted that claims 4, 5, 7, 10, and 11 are allowable over Perlman for the same reasons as set forth above with respect to claim 1.

Regarding claims 2, 6, 8, and 12, these claims are dependent upon independent claim 1, 4, 5, 7, 10, or 11. Thus, since independent claims 1, 4, 5, 7, 10, and 11 should be allowable as discussed above, claims 2, 6, 8, and 12 should also be allowable at least by virtue of their dependency on independent claim 1, 4, 5, 7, 10, or 11. Moreover, these claims recite additional features which are not disclosed, or even suggested, by the cited references taken either alone or in combination. For example, claim 2 recites "not allowing encrypted data to pass when it is determined that the first encryption key is not received," and claim 8 recites "an encrypted data blocker for not allowing encrypted data to pass when it is determined that the first encryption key is not received." Perlman fails to disclose, or even suggest, such claimed features.

In view of the foregoing, it is respectfully requested that the aforementioned anticipation rejection of claims 1, 2, 4-8, and 10-12 be withdrawn.

II. THE OBVIOUSNESS REJECTION OF CLAIMS 1, 2, 4-6, 19, and 20

On page 10 of the Decision on Appeal, the rejection of claims 3 and 9 under 35 U.S.C. § 103(a) as being unpatentable over Perlman in view of Ylonen et al. (U.S. Patent No. 6,438,612, hereinafter "Ylonen") was affirmed. In light of the current amendments to independent claims 1, 4, 5, 7, 10, and 11, this affirmation of the rejection is hereby respectfully traversed.

Under 35 U.S.C. § 103, the Patent Office bears the burden of establishing a prima facie case of obviousness. In re Fine, 837 F.2d 1071, 1074 (Fed. Cir. 1988). There are four separate factual inquiries to consider in making an obviousness determination: (1) the scope and content of the prior art; (2) the level of ordinary skill in the field of the invention; (3) the differences between the claimed invention and the prior art; and (4) the existence of any objective evidence, or "secondary considerations," of non-obviousness. Graham v. John Deere Co., 383 U.S. 1, 17-18 (1966); see also KSR Int'l Co. v. Teleflex Inc., 127 S. Ct. 1727 (2007). An "expansive and flexible

approach" should be applied when determining obviousness based on a combination of prior art references. KSR, 127 S. Ct. at 1739. However, a claimed invention combining multiple known elements is not rendered obvious simply because each element was known independently in the prior art. Id. at 1741. Rather, there must still be some "reason that would have prompted" a person of ordinary skill in the art to combine the elements in the specific way that he or she did. Id.; In re Icon Health & Fitness, Inc., 496 F.3d 1374, 1380 (Fed. Cir. 2007). Also, modification of a prior art reference may be obvious only if there exists a reason that would have prompted a person of ordinary skill to make the change. KSR, 127 S. Ct. at 1740-41.

It is respectfully submitted that the obviousness rejection of claims 3 and 9 has become moot in view of the deficiencies of the primary reference Perlman as discussed above with respect to independent claims 1 and 7, respectively. That is, claims 3 and 9 are dependent upon independent claims 1 and 7, respectively, and thus inherently incorporate all of the limitations of independent claims 1 and 7, respectively. Also, the secondary reference Ylonen fails to disclose, or even suggest, the deficiencies of the primary reference Perlman as discussed above with respect to independent claims 1 and 7. Thus, the combination of the secondary reference Ylonen with the primary

reference Perlman also fails to disclose, or even suggest, the deficiencies of the primary reference Perlman as discussed above with respect to independent claims 1 and 7. Accordingly, claims 3 and 9 should be allowable over the combination of the secondary reference Ylonen with the primary reference Perlman at least by virtue of their dependency on independent claims 1 and 7. Moreover, claims 3 and 9 recite additional features which are not disclosed, or even suggested, by the cited references taken either alone or in combination. For example, claims 3 and 9 recite "detecting an exchange of a first encryption key by monitoring Internet Key Exchange (IKE) protocol data traffic to determine whether the first encryption key is exchanged." Perlman and Ylonen either alone or in combination, fail to disclose, or even suggest, such claimed features, particularly when viewed in combination with the features of independent claims 1 and 7.

Even assuming, for the sake of argument, that Ylonen cures the deficiencies of Perlman, Applicants respectfully submit that the Office Action does not present a proper rationale to combine the references to achieve the claimed system and method, and thus has failed to set forth a *prima facie* case of obviousness.

Specifically, the Office asserts that modifying Perlman to include the alleged Internet Key Exchange (IKE) protocol data

feature of Ylonen would have been obvious because the modification "offers the advantage of using a key management scheme that provides authentication between source and destination while adhering to an industry standard method of key exchange." *See* Office Action at page 5. However, such a statement represents classic **impermissible hindsight**.

First, Applicants respectfully submit that the Office improperly ***assumes*** the combination recited in the claim would be desired. For example, the Examiner asserts that the combination "offers the *advantage* to...an industry standard method of key exchange" (emphasis added). *See* Office Action at p. 3. The PTO has the burden to establish that the prior art taken as a whole shows the desire or advantage. Here, the Office simply assumes (not the references as whole) that it would have been obvious to one of ordinary skill in the art to create an Internet Key Exchange (IKE) protocol data feature in Perlman's trusted network screening system. In addition, the Office fails to explain *why* the art as a whole would suggest such at least an Internet Key Exchange (IKE) protocol data feature specifically for a system that relies on a source or destination devices to initiate detection of key exchanges. Thus, Applicants submits that the Examiner's assumption is clearly improper.

Second, Applicants also submits that the Office's assertion of obviousness is lacking in ***evidence***. Instead, the Offce improperly relies on its own hindsight conjecture or improperly gleans from the Applicants' own specification. Furthermore, the Office's statement that Ylonen could provide such Internet Key Exchange (IKE) protocol data feature to Perlman's specific method and system is wholly unsupported. In fact, such reasons for obviousness cited by the Office to combine the references, especially that a such a combination is "advantageous," is nowhere to be found in either the Ylonen or Perlman reference. Even assuming, for the sake of argument, that the reason for obviousness is applicable, Perlman provides no support indicating that it would benefit from the teachings of Ylonen's alleged Internet Key Exchange (IKE) protocol data feature. For example, Perlman is concerned with services for screening network information from trusted sources, whereas Ylonen is primarily concerned with using IPsec security associations to help perform virtual routing. Therefore, a person of ordinary skill would not combine teachings from these disparate references to arrive at Applicants' invention.

In view of the foregoing, it is respectfully submitted that the combination of the primary reference Perlman with the secondary reference Ylonen fails to disclose, suggest, or render

obvious the elements of claims 3 and 9. Accordingly, it is respectfully submitted that claims 3 and 9 of the present application are not unpatentable over the combination of the primary reference Perlman with the secondary reference Ylonen. Thus, a prima facie case of obviousness against claims 3 and 9 of the present application has not been established.

In view of the foregoing, it is respectfully requested that the obviousness rejection of claims 3 and 9 be withdrawn.

II. CONCLUSION

In view of the foregoing, it is respectfully submitted that the present application is in condition for allowance, and an early indication of the same is courteously solicited. The Examiner is respectfully requested to contact the undersigned by telephone at the below listed telephone number, in order to expedite resolution of any issues and to expedite passage of the present application to issue, if any comments, questions, or suggestions arise in connection with the present application.

To the extent necessary, a petition for an extension of time under 37 CFR § 1.136 is hereby made.

Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to

Deposit Account No. 50-0206, and please credit any excess fees to the same deposit account.

Respectfully submitted,

Hunton & Williams LLP

By: _____
Thomas E. Anderson
Registration No. 37,063

TEA/GYW

Hunton & Williams LLP
1900 K Street, N.W.
Washington, D.C. 20006-1109
Telephone: (202) 955-1500
Facsimile: (202) 778-2201

Date: November 18, 2008